Federal Cyber Service: Scholarship for Service (SFS)

A Federal Cyber Service Training and Education Initiative

Program Solicitation

NSF 01-11

DIRECTORATE FOR EDUCATION AND HUMAN RESOURCES
DIVISION OF UNDERGRADUATE EDUCATION

DEADLINES: **Letters of Intent (optional): December 13, 2000**
Proposals: January 24, 2001

NATIONAL SCIENCE FOUNDATION

The National Science Foundation promotes and advances scientific progress in the United States by competitively awarding grants and cooperative agreements for research and education in the sciences, mathematics, and engineering.

To get the latest information about program deadlines, to download copies of NSF publications, and to access abstracts of awards, visit the NSF Web Site at:

http://www.nsf.gov

• **Location:**	4201 Wilson Blvd. Arlington, VA 22230
• **For General Information (NSF Information Center):**	(703) 292-5111
• **TDD (for the hearing-impaired):**	(703) 292-5090
• **To Order Publications or Forms:**	
Send an e-mail to:	pubs@nsf.gov
or telephone:	(301) 947-2722
• **To Locate NSF Employees:**	(703) 292-5111

SUMMARY OF PROGRAM REQUIREMENTS

GENERAL INFORMATION

Program Title: Federal Cyber Service: Scholarship for Service (SFS)

Synopsis of Program:

The Federal Cyber Service: Scholarship for Service (SFS) program seeks to increase the number of qualified students entering the fields of information assurance and computer security and to increase the capacity of the United States higher education enterprise to continue to produce such professionals in these fields to meet the needs of our increasingly technological society. The SFS program is composed of three tracks:

Scholarship Track

The Scholarship Track provides funding to colleges and universities for scholarships in information assurance and computer security fields. A typical scholarship grant will provide up to four years of institutional funding to support two-year scholarships for up to 3 cohorts of up to 10 students. A typical award might support 3 cohort classes of 10 first-year students (year 1), 10 first-year and 10 second-year students (year 2), 10 first-year and 10 second-year students (year 3), and 10 second-year students (year 4). These students shall pursue academic programs in information assurance for the Junior and Senior years of undergraduate study or for two years of Masters level study. These students will participate as a cohort during two years of study and activities, including a summer internship in a federal agency at the end of their first year of study. The recipients of the scholarships will become part of the Federal Cyber Service of information technology specialists whose responsibility is to ensure the protection of the United States Government information infrastructure. Upon graduation after their two-year scholarships, recipients will be required to work for a federal agency for two years as their Federal Cyber Service commitment. The scholarships provide academic year stipends of $8,000 per year for undergraduate students and $12,000 per year for graduate students. Grantee institutions may request up to $50,000 per year toward the support of faculty dedicated to this program.

Capacity Building: Faculty Development Track

The Faculty Development Track will provide funds for faculty development in the area of information assurance and computer security. Funding for up to $100,000 per year for 2 years is available for CAE/IAE certified or equivalent institutions to conduct regional and national faculty development seminars for faculty teams from non-CAE/IAE institutions.

Capacity Building: Institutional Development Track

The Institutional Development Track will provide funds for institutional development in the area of information assurance and computer security. Funding for up to $100,000 per year for 2 years is available for institutions not currently eligible for the SFS Scholarship Track to develop institutional capacity in the information assurance and computer security area.

Cognizant Program Officer: Harriet Taylor, Program Director, DUE, e-mail: htaylor@nsf.gov

Applicable Catalog of Federal Domestic Assistance (CFDA) Number: 47.076 -- Education and Human Resources

ELIGIBILITY INFORMATION

- **Organization Limit:**

  - **Scholarship Track:** Proposals are invited from accredited U.S. institutions of higher education with strong programs of activity in information assurance with Center of Excellence in Information Assurance Education (CAE/IAE) certification, or an approved equivalent program. The institution must be able to demonstrate that its programs meet criteria equivalent to those necessary for certification by the National Security Agency as a Center of Academic Excellence in Information Assurance Education (please see http://www.nsa.gov/isso/programs/nietp/newspg1.htm to see if your program has the equivalent qualifications).

  - **Capacity Building - Faculty Development Track:** Proposals are invited from accredited U.S. institutions of higher education or consortia with strong programs of activity in information assurance with Center of Excellence in Information Assurance Education (CAE/IAE) certification, or an approved equivalent program. The institution (lead institution in consortia) must be able to demonstrate that its programs meet criteria equivalent to those necessary for certification by the National Security Agency as a Center of Academic Excellence in Information Assurance Education (please see http://www.nsa.gov/isso/programs/nietp/newspg1.htm to see if your program has the equivalent qualifications).

  - **Capacity Building - Institutional Development Track:** Proposals are invited from accredited U.S. institutions of higher education or consortia with strong programs of activity in information assurance who do not have Center of Excellence in Information Assurance Education (CAE/IAE) certification, or an approved equivalent program.

- **PI Eligibility Limit:** None

- **Limit on Number of Proposals:** An institution may submit no more than one proposal per track per competition.

AWARD INFORMATION

- **Anticipated Type of Award:** Standard Grant or Continuing Grant

- **Estimated Number of Awards:** 5-8 in the Scholarship Track, 1-3 in the Capacity Building: Faculty Development track, and 2-5 in the Capacity Building: Institutional Development track

- **Anticipated Funding Available:** $11 million, pending availability of funding

PROPOSAL PREPARATION AND SUBMISSION INSTRUCTIONS

A. Proposal Preparation Guidelines

- **Proposal Preparation Instructions:** Standard Preparation Guidelines

  - Standard Grant Proposal Guide instructions apply

B. Budgetary Information

- **Cost Sharing Requirements:** There must be a 1:1 dollar match for any equipment requested under the Capacity Building: Institutional Development Track.

- **Indirect (F&A) Limitations:** No indirect costs may be charged on scholarship grants, but grantee institutions may request up to 8 percent of the total budget to address the management and administrative costs associated with operating the SFS scholarship program. Institutions may also request up to 2 percent of the total budget to address curriculum, laboratory, and faculty development in support of the SFS program. Funds requested for management and administrative costs as well as for curriculum, laboratory, and faculty development must be included in standard budget categories in the proposal budget and appropriate justification must be provided in the budget explanation. Indirect costs may be charged on non-participant and non-equipment costs on grants in the Faculty Development and Institutional Development Tracks.

- **Other Budgetary Limitations:** The Scholarship Track provides academic year stipends of $8,000 per year for undergraduate students and $12,000 per year for graduate students. Grantee institutions may request up to $50,000 per year toward the support of faculty dedicated to this program. The Faculty Development Track provides funding for up to $100,000 per year for 2 years to CAE/IAE certified or equivalent institutions. The Institutional Development Track provides funding for up to $100,000 per year for 2 years is available for institutions not currently eligible for the SFS Scholarship Track to develop institutional capacity in the information assurance and computer security area

C. Deadline/Target Dates

- **Letter of Intent Deadline:** Letter of intent is requested by all three tracks, but not required, by December 13, 2000, transmitted by e-mail to <sfs@nsf.gov>.

- **Preproposal Deadline:** None

- **Full Proposal Deadline:** January 24, 2001, by 5:00 PM submitter's local time

SFS Program Deadlines by Track			
Track	**Letter of Intent**	**Proposal**	**Award Date (anticipated)**
Scholarship	December 13, 2000	January 24, 2001	June 2001
Capacity Building: Faculty Development	December 13, 2000	January 24, 2001	June 2001
Capacity Building: Institutional Development	December 13, 2000	January 24, 2001	June 2001

D. FastLane Requirements

- **FastLane Submission:** Full Proposal Required
- **Fast Lane Contact:** FastLane Help Desk, telephone: (800) 673-6188, e-mail <fastlane@nsf.gov>. Teresa Neely, Computer Specialist, Division of Undergraduate Education, Room 835, telephone: (703) 292-4631, e-mail <duefl@nsf.gov>.

PROPOSAL REVIEW INFORMATION

- **Merit Review Criteria:** Additional merit review criteria apply. Please see the full program announcement for further information.

AWARD ADMINISTRATION INFORMATION

- **Award Conditions:** Standard award conditions apply and special conditions related to the unique requirements of this program.
- **Reporting Requirements:** Additional reporting requirements apply. Please see the full program announcement for further information.

I. INTRODUCTION

The Federal Cyber Service: Scholarship for Service (SFS) program anticipates providing funding to colleges and universities for scholarships, capacity building as faculty development, and capacity building as institutional development in information assurance and computer security fields. A typical scholarship grant will provide four years of funding to enable the institution to cover as many as to three cohorts of up to 10 two -year full scholarships (30 two-year scholarships total during the grant period) for study leading to baccalaureate and masters degrees providing technical competence in the area of information assurance and security. A typical capacity building grant will provide funds for institutional development or for faculty development in the area of information assurance and computer security. The program is established by the National Science Foundation (NSF) in accordance with the Federal Cyber Service Training and Education Initiative as described in the President's *National Plan for Information Systems Protection*. This initiative reflects the critical need for Information Technology (IT) professionals specializing in information assurance and security. The expected outcomes of this program include:

- New entrants to the federal workforce with the education and training that will enhance the security of critical federal information infrastructure,
- An increased national capability for the education of IT professionals in critical information infrastructure protection disciplines,
- Increased national research and development capabilities in critical information infrastructure protection,
- Strengthened partnerships between institutions of higher education and relevant employment sectors.

The scholarship program provides funding for two-year full scholarships to pursue academic programs in information assurance for the Junior and Senior years of undergraduate study or for two years of masters-level study. Upon graduation the recipients of the scholarships will become part of the Federal Cyber Service of information technology specialists whose responsibility is to ensure the protection of the United States Government's information infrastructure. After their two-year scholarships, the recipients will be required to work for a federal agency for two years as their Federal Cyber Service commitment.

II. PROGRAM DESCRIPTION

The primary objective of the SFS program is to build information assurance capacity and to provide an educated cadre of information technology professionals who can help assure the protection of the United States Government information infrastructure. The three tracks in this program are described below.

Scholarship Track:

The SFS program provides funds to colleges and universities for student scholarships in support of education in information technology areas relevant to information assurance and computer security. In return for their scholarships and stipend, students must agree to work after graduation for two years as an information assurance specialist in the Federal Cyber Service for a federal agency.

During the scholarship period, the students will participate in internships at federal agencies and participate in other Scholarship for Service activities such as conferences, workshops, and seminars. These activities are aimed at developing a community of practice that will enhance their individual and collective skills in an area increasingly important to the health and safety of the United States. The Office of Personal Management (OPM) will partner with the NSF in this program by providing the internships at Federal agencies and Federal agency placement after graduation. The OPM will also be responsible for the hiring of students as Federal employees, for ensuring that contractual obligations are met by the students during their scholarship period and after graduation, and for assessing whether the program helps meet the personnel needs of the Federal government for information infrastructure protection.

Grantee institutions will establish a scholarship activity under the SFS program. Scholarship support will be provided to students who compete successfully in a selection process developed by the grantee, who meet the SFS eligibility criteria, and who are selected as qualified for employment in the Federal Cyber Service by the OPM. It is expected that scholarship participants will receive their degree (undergraduate or masters) within two years of the beginning of their scholarships. Each proposing institution will provide a description of their selection criteria and process, and explain and justify the proposed distribution of scholarship recipients. In particular, institutions must ensure that groups underrepresented in information technology have fair access to scholarships.

In order to increase information security expertise and capacity at institutions serving underrepresented populations, application by and partnerships with minority serving institutions is encouraged. The U. S. Department of Education's Office of Civil Rights maintains a list of Accredited Postsecondary Minority Institutions <http://www.ed.gov/offices/OCR/2000minorityinst.html>, which may assist proposers in determining whether their institutions fall in this category.

The SFS scholarship eligibility criteria for students are

- United States citizens
- Full time student within two years of graduation in a Computer Security or Information Assurance program at an awardee institution.

Students identified by their institutions for scholarships must meet selection criteria for federal employment. In addition, internship placements and final job placements may require security

clearances. Scholarship recipients maybe required to undergo the background investigation required to obtain such clearances.

The selection process for scholarship recipients should include indicators of academic merit and other indicators of future professional success. Multiple indicators may be appropriate in gauging both academic merit (e.g., grade point average, class rank) and professionalism (e.g., motivation, ability to manage time and resources, communication skills). Selection criteria should be flexible enough to accommodate applicants who come from diverse backgrounds and with diverse career goals. Federal Cyber Service scholars must continue to demonstrate their eligibility in each semester/quarter of SFS support. Proposals must clearly describe the selection criteria to be used.

Awardee institutions must submit their lists of candidates for SFS scholarships to OPM for final approval and selection. OPM will manage the scholars' internships and job placements. OPM will also manage compliance with the mandatory employment component of this program.

It is expected that grantee institutions will provide the infrastructure to recruit and support students that is necessary for the successful graduation of scholarship recipients. Such an infrastructure might include, for example:

- Recruitment of students, with special consideration to groups underrepresented in SFS fields. (i.e., women, racial and ethnic minorities, and persons with disabilities).
- Academic support and mentoring to support students in making progress toward the degree, and to prepare students for the workplace.
- Application-oriented experiences to increase the students' understanding of information assurance needs and their relationship to educational preparation.
- Retention of scholarship recipients to degree.

Grantee institutions are also expected to have clearly articulated management and administrative plans for the following program elements. These items must be clearly detailed in the budget justification of the proposal. Verification of scholarship candidates' eligibility, including the recipients' academic merit, appropriate affective skills, and enrollment in a certified or equivalent information assurance program.

- Provision of scholarship amounts to be used for expenses normally incurred by full-time students in the institution, including tuition, room and board, and equipment. These shall be included in participant support costs.
- Provision of academic year stipends of $8,000 per year for undergraduate students and $12,000 per year for graduate students. These charges shall be included in participant support costs.
- Provision for coordination with OPM for summer intern placements for each student. Students are expected to take Federal intern positions in the summer between their first and second year of scholarship study. The payments for summer internships will take place outside the university grant structure and are not to be included in the budget.

- Provisions for tracking the academic progress of students to determine their continued eligibility throughout the academic part of the program. Subsequent tracking of students to verify that they meet the service obligation will be done by OPM.
- Evaluation of program outcomes.
- Demonstration of ability to partner with the OPM in student hiring and agency placement.
- Plan for professional development of academic staff.

Grantee institutions may request up to $50,000 per year toward the support of faculty dedicated to this program.

No indirect costs may be charged on scholarship grants, but grantee institutions may request up to 8 percent of the total budget to address the management and administrative costs associated with operating the SFS scholarship program. Institutions may also request up to 2 percent of the total budget to address curriculum, laboratory, and faculty development in support of the SFS program. Funds requested for management and administrative costs as well as for curriculum, laboratory, and faculty development must be included in standard budget categories in the proposal budget and appropriate justification must be provided in the budget explanation. Collaborations with industry, non-profit, or state organizations are strongly encouraged in the institutional and faculty development activities to provide additional support for students not chosen for the scholarships to participate in student internships and in Federal Cyber Service activities.

The Principal Investigator (PI) will have overall responsibility for the administration of the institution's grant award, the management of the project, and interactions with the NSF and OPM. The PI and the grantee institution are expected to have or to develop an administrative structure that enables faculty, academic administrators, scholarship recipients, and others involved in the project to interact productively during the grant award period. The PI is expected to be an integral participant in the educational activities of the SFS project. The management plan will be an integral part of the proposal evaluation.

Within the grantee institution, the departments making up the Center of Academic Excellence in Information Assurance Education or equivalent are expected to collaborate in implementing the project plans. To broaden the support of their activities, proposers are encouraged to establish collaborative arrangements with other organizations.

Proposing institutions must have strong programs of activity in information assurance with Center of Excellence in Information Assurance Education (CAE/IAE) certification, or an approved equivalent program. The institution must be able to demonstrate that its programs meet criteria equivalent to those necessary for certification by the National Security Agency as a Center of Academic Excellence in Information Assurance Education. Additionally, they must demonstrate their continuing commitment to faculty development in information assurance and continuing commitment to curriculum excellence in information assurance. Proposals should contain documentation of CAE/IAE certification or demonstrate how the program meets the criteria published by the National Security Agency at http://www.nsa.gov/isso/programs/nietp/newspg1.htm.

Proposals should clearly describe the plan for implementing a program with the goals and characteristics outlined in the preceding text. The proposal should include the design of activities to be undertaken, a description of the processes through which the program elements will be implemented, and plans for documentation. The proposal should clearly describe the student-support structure, plans to manage and administer the program, and evidence of the quality of the institution's educational program in Information Assurance.

Capacity Building:

The SFS program provides for capacity building in information assurance and computer security fields by providing funds in two areas, Faculty Development and Institutional Development.

Capacity Building: Faculty Development:

Funding for up to $100,000 per year for 2 years is available for CAE/IAE certified or equivalent institutions to conduct regional and national faculty development seminars for faculty teams from non-CAE/IAE institutions. Grants are made for the development and implementation of activities that assist faculty to learn about recent advances in information assurance and computer security to improve their instructional capability in these areas. The SFS program seeks projects that provide faculty teams with opportunities for continued professional growth in areas related to information assurance and computer security. Such projects typically include conferences, workshops, intensive seminars, distance learning opportunities, or a combination of such activities to bring about the desired professional development for faculty. These activities typically last from a few days to several weeks and are usually conducted in the summer, with follow-up activities during the academic year. To effect long-term change, projects for faculty enhancement should normally span at least two academic years.

Projects must describe how faculty participants will be recruited, what level of support will be provided for participants, what evaluation procedures will be used, and the type of follow-up provided for participants as they implement new courses and curriculum in information assurance and computer security. Projects must also describe how the institutional teams of two or more members must be formed and the institutional support evidence that participating institutions must provide to assure that these teams can continue to work towards building institutional capacity once the team completes its faculty development activities.

Institutional indirect costs may be charged against all costs, except participant costs. No equipment costs may be included in these proposals.

Capacity Building: Institutional Development:

Funding for up to $100,000 per year for 2 years is available for institutions not currently eligible for the SFS Scholarship Track to develop institutional capacity in the information assurance and computer security area. Minority serving institutions are particularly encouraged to submit proposals in this area. This area encourages proposals to do the following:

- *Adaptation and Implementation*: The program wishes to foster collaboration and dialogue among institutions offering courses and programs in information assurance. Consequently, the SFS program supports proposals for the adaptation and implementation of exemplary educational materials, courses, and curricula that have been developed at CAE/IAE or comparable institutions to promote

the increased educational capacity in information assurance and computer security education programs.

- *Curriculum and Educational Materials Development*: Supported activities should affect the learning environment, course content, and the experience of instruction. Projects often result in textbooks, laboratory experiments and manuals, software, CD-ROMS, videos, and other courseware. Such products are expected to be widely disseminated through commercial publishers, conferences, workshops, electronic networks, journal articles, and other means. A project's focus may range from the substantial revision of existing instructional materials to the creation of entirely new ones; from a few modules at a single educational level to comprehensive curriculum for multiple years; and from a single subject to the integration of several disciplines.

- *Technical Experiences*: Well-designed technical experiences in the classroom and in a work environment can give students and faculty a broad, up-to-date, real-world perspective on the information assurance fields. Such experiences typically allow participants to get hands-on exposure to the field and thereby gain confidence in their abilities in technical areas; interact closely with computer security experts; obtain information about various careers available in information assurance and computer security; become aware of academic preparation necessary for such careers; and become acquainted with the environments of other academic institutions, private industry, and government agencies.

  Projects providing technical experiences may consist of any combination of activities involving instruction, problem solving, research, deployment of security solutions, and industrial internships. Proposals should describe recruitment strategies; criteria for selection of participants; and the relevance of the planned experiences to the goal of developing expertise in information assurance and computer security.

- *Laboratory Development*: Laboratory or field experiences using suitable modern instrumentation are crucial elements in advanced technology fields. The SFS program supports the development of innovative methods for using laboratory and field exercises to improve students' understanding of basic principles. It also supports use by faculty of modern instrumentation, new technologies, or applications of instruments that extend their instructional capability. The program also encourages the establishment of equipment-sharing arrangements through consortia of institutions developing capacity in information assurance and computer security.

  Funds requested for equipment and other technology must not exceed $100,000 of the total request and must be matched by non-Federal funds, equipment, or technology with a value equal to the funds requested from NSF. Indirect costs may be charged against all costs related to these proposals except for equipment costs.

III. ELIGIBILITY INFORMATION

Accredited U.S. institutions of higher education and consortia with strong programs of activity in information assurance are eligible to apply for the Scholarship and Faculty Development tracks. The institution (lead institution in consortia) must be able to demonstrate that its programs meet criteria equivalent to those necessary for certification by the National Security Agency as a Center of Academic Excellence in Information Assurance Education (please see http://www.nsa.gov/isso/programs/nietp/newspg1.htm to see if your program has the equivalent qualifications).

IV. AWARD INFORMATION

The SFS Scholarship track supports a university or college based scholarship program that supports two years of tuition, room and board, and stipend for students in the general area of information assurance and security. The program contains an internship component intended to support hands-on training in the Federal Government that is supported through the award for the internships and other training. A typical award might be approximately $2.5 million for four years supporting three cohort classes of 10 first-year students (year 1), 10 first-year and 10 second-year students (year 2), 10 first-year and 10 second-year students (year 3), and 10 second-year students (year 4). The total award sizes will depend upon the tuition and room and board costs and on the cost of faculty development.

V. PROPOSAL PREPARATION AND SUBMISSION INSTRUCTIONS

A. Letter of Intent

A letter of intent to submit a proposal is requested (but not required) from all applicants, to assist NSF in planning for review. The letter of intent is not a preliminary proposal. It is a brief statement detailing the submitting institution and any partners, track (Scholarship, Capacity Building: Faculty Development or Capacity Building: Institutional Development), and a short description of the project. It should be received at NSF no later than December 13, 2000. Letters of intent must be sent by electronic mail to <sfs@nsf.gov>.

B. Proposal Preparation Instructions

Proposals submitted in response to this program announcement should be prepared and submitted in accordance with the general guidelines contained in the NSF *Grant Proposal Guide* (GPG) (NSF 01-2). The complete text of the GPG is available electronically on the NSF Web site at: http://www.nsf.gov/cgi-bin/getpub?gpg. Paper copies of the GPG may be obtained from the NSF Publications Clearinghouse, telephone (301) 947-2722 or by e-mail from <pubs@nsf.gov>.

Proposers are reminded to identify the program announcement number in the program announcement/solicitation block on the NSF Form 1207, *Cover Sheet For Proposal to the National Science Foundation.* Compliance with this requirement is critical to determining the relevant proposal processing guidelines. Failure to submit this information may delay processing.

C. Cost Sharing Requirements

Any equipment costs in proposals must have a 1:1 cost sharing match from the institution and must be shown on Line M of the NSF Form 1030.

D. Deadline/Target Dates

Investigators intending to submit proposals should submit an e-mail letter of intent (optional) to <sfs@nsf.gov> by 5:00 PM local time, December 13, 2000. Proposals submitted in response to this announcement must be submitted by 5:00 PM, local time, January 24, 2001.

E. FastLane Requirements

Proposers are required to prepare and submit all proposals for this Program Solicitation through the FastLane system. Detailed instructions for proposal preparation and submission via FastLane are available at: https://www.fastlane.nsf.gov/a1/newstan.htm. For FastLane user support, call 1-800-673-6188.

Submission of Signed Cover Sheets. The signed copy of the proposal Cover Sheet (NSF Form 1207) must be postmarked (or contain a legible proof of mailing date assigned by the carrier) within five working days following proposal submission and be forwarded to the following address:

National Science Foundation
DIS – FastLane Cover Sheet
4201 Wilson Blvd.
Arlington, VA 22230

VI. PROPOSAL REVIEW INFORMATION

A. NSF Proposal Review Process

Reviews of proposals submitted to NSF are solicited from peers with expertise in the substantive area of the proposed research or education project. These reviewers are selected by Program Officers charged with the oversight of the review process. NSF invites the proposer to suggest at the time of submission the names of appropriate or inappropriate reviewers. Care is taken to ensure that reviewers have no conflicts with the proposer. Special efforts are made to recruit reviewers from non-academic institutions, minority-serving institutions, or adjacent disciplines to that principally addressed in the proposal.

Proposals will be reviewed against the following general review criteria established by the National Science Board. Following each criterion are potential considerations that the reviewer may employ in the evaluation. These are suggestions and not all will apply to any given proposal. Each reviewer will be asked to address only those that are relevant to the proposal and for which he/she is qualified to make judgements.

What is the intellectual merit of the proposed activity?

How important is the proposed activity to advancing knowledge and understanding within its own field or across different fields? How well qualified is the proposer (individual or team) to conduct the project? (If appropriate, the reviewer will comment on the quality of the prior work.) To what extent does the

proposed activity suggest and explore creative and original concepts? How well conceived and organized is the proposed activity? Is there sufficient access to resources?

What are the broader impacts of the proposed activity?

How well does the activity advance discovery and understanding while promoting teaching, training, and learning? How well does the proposed activity broaden the participation of underrepresented groups (e.g., gender, ethnicity, disability, geographic, etc.)? To what extent will it enhance the infrastructure for research and education, such as facilities, instrumentation, networks, and partnerships? Will the results be disseminated broadly to enhance scientific and technological understanding? What may be the benefits of the proposed activity to society?

Review Criteria Specific to the SFS program

Reviewers will be asked to consider the merit review criteria with emphasis placed on the SFS program components (see "Program Description"). These include:

- The quality and completeness of the management and administrative plan. The plan must address all elements expressed in the program solicitation,
- Designation as a Center of Academic Excellence in Information Assurance Education or approved equivalent programs (Scholarship and Faculty Development tracks),
- Quality of education and research in Information Assurance at the institution and the extent which education and research are integrated,
- Application-oriented experiences to increase the student's understanding of information assurance needs and their relationship to educational practices,
- Faculty member with specific expertise in information assurance and security as well as professional development for other faculty,
- Discipline faculty members integrally involved with the scholarship students and working with the students as a cohort, and
- For the scholarship track, the review may also consider the provision for appropriate student support infrastructure for the successful graduation of scholarship recipients as expressed in the program announcement.

Principal Investigators should address the following elements in their proposal to provide reviewers with the information necessary to respond fully to both of the above-described NSF merit review criteria. NSF staff will give these elements careful consideration in making funding decisions.

Integration of Research and Education

One of the principal strategies in support of NSF's goals is to foster integration of research and education through the programs, projects, and activities it supports at academic and research institutions. These institutions provide abundant opportunities where individuals may concurrently

assume responsibilities as researchers, educators, and students and where all can engage in joint efforts that infuse education with the excitement of discovery and enrich research through the diversity of learning perspectives.

Integrating Diversity into NSF Programs, Projects, and Activities

Broadening opportunities and enabling the participation of all citizens - women and men, underrepresented minorities, and persons with disabilities - is essential to the health and vitality of science and engineering. NSF is committed to this principle of diversity and deems it central to the programs, projects, and activities it considers and supports.

A summary rating and accompanying narrative will be completed and signed by each reviewer. In all cases, reviews are treated as confidential documents. Verbatim copies of reviews, excluding the names of the reviewers, are mailed to the Principal Investigator/Project Director by the Program Director. In addition, the proposer will receive an explanation of the decision to award or decline funding.

B. Review Protocol and Associated Customer Service Standard

All proposals are carefully reviewed by at least three other persons outside NSF who are experts in the particular field represented by the proposal. Proposals submitted in response to this solicitation will be reviewed by Panel Review.

Reviewers will be asked to formulate a recommendation to either support or decline each proposal. The Program Officer assigned to manage the proposal's review will consider the advice of reviewers and will formulate a recommendation.

NSF will be able to tell applicants whether their proposals have been declined or recommended for funding within six months for 95 percent of proposals. The time interval begins on the proposal deadline or target date or from the date of receipt, if deadlines or target dates are not used by the program. The interval ends when the Division Director accepts the Program Officer's recommendation.

In all cases, after programmatic approval has been obtained, the proposals recommended for funding will be forwarded to the Division of Grants and Agreements for review of business, financial, and policy implications and the processing and issuance of a grant or other agreement. Proposers are cautioned that only a Grants and Agreements Officer may make commitments, obligations or awards on behalf of NSF or authorize the expenditure of funds. No commitment on the part of NSF should be inferred from technical or budgetary discussions with a NSF Program Officer. A Principal Investigator or organization that makes financial or personnel commitments in the absence of a grant or cooperative agreement signed by the NSF Grants and Agreements Officer does so at its own risk.

VII. AWARD ADMINISTRATION INFORMATION

A. Notification of the Award

Notification of the award is made to *the submitting organization* by a Grants Officer in the Division of Grants and Agreements. Organizations whose proposals are declined will be advised as promptly as possible by the cognizant NSF Program Division administering the program. Verbatim copies of reviews, not including the identity of the reviewer, will be provided automatically to the Principal Investigator. (See section VI. A, for additional information on the review process).

B. Award Conditions

An NSF award consists of: (1) the award letter, which includes any special provisions applicable to the award and any numbered amendments thereto; (2) the budget, which indicates the amounts, by categories of expense, on which NSF has based its support (or otherwise communicates any specific approvals or disapprovals of proposed expenditures); (3) the proposal referenced in the award letter; (4) the applicable award conditions, such as Grant General Conditions (NSF-GC-1)* or Federal Demonstration Partnership (FDP) Terms and Conditions * and (5) any NSF brochure, program guide, announcement or other NSF issuance that may be incorporated by reference in the award letter.

*These documents may be accessed electronically on NSF's web site at http://www.nsf.gov/home/grants/grants_gac.htm. Paper copies may be obtained from the NSF Publications Clearinghouse, telephone (301) 947-2722 or by e-mail from pubs@nsf.gov.

More comprehensive information on NSF Award Conditions is contained in the NSF *Grant Policy Manual* (GPM) Chapter II, (NSF 95-26) available electronically on the NSF web site at http://www.nsf.gov/cgi-bin/getpub?gpm. The GPM is also for sale through the Superintendent of Documents, Government Printing Office (GPO), Washington, DC 20402. The telephone number at GPO for subscription information is (202) 512-1800. The GPM may be ordered through the GPO web site at http://www.gpo.gov.

C. Reporting Requirements

For all multi-year grants (including both standard and continuing grants), the PI must submit an annual project report to the cognizant Program Officer at least 90 days before the end of the current budget period.

The institutions must report annually on the academics of scholarship students in the program including the numbers of students making good progress, dropout rates from the program, and developments in Information Assurance curricula in the scholarship program.

Within 90 days after the expiration of an award, the PI also is required to submit a final project report. Approximately 30 days before expiration, NSF will send a notice to remind the PI of the requirement to file the final project report. Failure to provide final technical reports delays NSF review and processing of pending proposals for that PI. PIs should examine the formats of the required reports in advance to assure availability of required data.

NSF has implemented an electronic project reporting system, available through FastLane. This system permits electronic submission and updating of project reports, including information on: project participants (individual and organizational); activities and findings; publications; and other specific products and contributions. PIs will not be required to re-enter information previously provided, either with a proposal or in earlier updates using the electronic system.

VIII. CONTACTS FOR ADDITIONAL INFORMATION

General inquiries should be made to the Federal Cyber Service: Scholarships for Service Program:

Harriet Taylor, Program Officer
Division of Undergraduate Education
National Science Foundation
4201 Wilson Blvd., Suite 835
Arlington, VA 22230
Telephone (703) 292-4642
E-mail: htaylor@nsf.gov

For questions related to use of FastLane, contact NSF's FastLane Help Desk, telephone 1-800-673-6188, e-mail fastlane@nsf.gov; or Teresa Neely, Division of Undergraduate Education, telephone (703) 292-4631, e-mail duefl@nsf.gov.

IX. OTHER PROGRAMS OF INTEREST

Information about the Computer Science, Engineering, and Mathematics Scholarships (CSEMS) program is available at http://www.ehr.nsf.gov/EHR/DUE/programs/csems/

The NSF Guide to Programs is a compilation of funding for research and education in science, mathematics, and engineering. The NSF Guide to Programs is available electronically at http://www.nsf.gov/cgi-bin/getpub?gp. General descriptions of NSF programs, research areas, and eligibility information for proposal submission are provided in each chapter.

Many NSF programs offer announcements concerning specific proposal requirements. To obtain additional information about these requirements, contact the appropriate NSF program offices. Any changes in NSF's fiscal year programs occurring after press time for the Guide to Programs will be announced in the NSF E-Bulletin, which is updated daily on the NSF web site at http://www.nsf.gov/home/ebulletin, and in individual program announcements/solicitations. Subscribers can also sign up for NSF's Custom News Service (http://www.nsf.gov/home/cns/start.htm) to be notified of new funding opportunities that become available.

ABOUT THE NATIONAL SCIENCE FOUNDATION

The National Science Foundation (NSF) funds research and education in most fields of science and engineering. Awardees are wholly responsible for conducting their project activities and preparing the results for publication. Thus, the Foundation does not assume responsibility for such findings or their interpretation.

NSF welcomes proposals from all qualified scientists, engineers and educators. The Foundation strongly encourages women, minorities and persons with disabilities to compete fully in its programs. In accordance with Federal statutes, regulations and NSF policies, no person on grounds of race, color, age, sex, national origin or disability shall be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving financial assistance from NSF (unless otherwise specified in the eligibility requirements for a particular program).

Facilitation Awards for Scientists and Engineers with Disabilities (FASED) provide funding for special assistance or equipment to enable persons with disabilities (investigators and other staff, including student research assistants) to work on NSF-supported projects. See the program announcement/solicitation for further information.

The National Science Foundation has Telephonic Device for the Deaf (TDD) and Federal Information Relay Service (FIRS) capabilities that enable individuals with hearing impairments to communicate with the Foundation about NSF programs, employment or general information. TDD may be accessed at (703) 292-5090, FIRS at 1-800-877-8339.

The National Science Foundation is committed to making all of the information we publish easy to understand. If you have a suggestion about how to improve the clarity of this document or other NSF-published materials, please contact us at plainlanguage@nsf.gov.

PRIVACY ACT AND PUBLIC BURDEN STATEMENTS

The information requested on proposal forms and project reports is solicited under the authority of the National Science Foundation Act of 1950, as amended. The information on proposal forms will be used in connection with the selection of qualified proposals; project reports submitted by awardees will be used for program evaluation and reporting within the Executive Branch and to Congress. The information requested may be disclosed to qualified reviewers and staff assistants as part of the proposal review process; to applicant institutions/grantees to provide or obtain data regarding the proposal review process, award decisions, or the administration of awards; to government contractors, experts, volunteers and researchers and educators as necessary to complete assigned work; to other government agencies needing information as part of the review process or in order to coordinate programs; and to another Federal agency, court or party in a court or Federal administrative proceeding if the government is a party. Information about Principal Investigators may be added to the Reviewer file and used to select potential candidates to serve as peer reviewers or advisory committee members. See Systems of Records, NSF-50, "Principal Investigator/Proposal File and Associated Records," 63 Federal Register 267 (January 5, 1998), and NSF-51, "Reviewer/Proposal File and Associated Records," 63 Federal Register 268 (January 5, 1998). Submission of the information is voluntary. Failure to provide full and complete information, however, may reduce the possibility of receiving an award.

Pursuant to 5 CFR 1320.5(b), an agency may not conduct or sponsor, and a person is not required to respond to an information collection unless it displays a valid OMB control number. The OMB control number for this collection is 3145-0058. Public reporting burden for this collection of information is estimated to average 120 hours per response, including the time for reviewing instructions. Send comments regarding this burden estimate and any other aspect of this collection of information, including suggestions for reducing this burden, to: Suzanne Plimpton, Reports Clearance Officer, Information Dissemination Branch, Division of Administrative Services, National Science Foundation, Arlington, VA 22230, or to Office of Information and Regulatory Affairs of OMB, Attention: Desk Officer for National Science Foundation (3145-0058), 725 - 17th Street, N.W. Room 10235, Washington, D.C. 20503.

NSF 01-11

OMB control number: 3145-0058